Constructions of Subspace Codes

Heide Gluesing-Luerssen

University of Kentucky

ALCOMA15, Kloster Banz

*Joint work Carolyn Troha.

Outline

1. Subspace Codes
2. A Linkage Construction
3. Construction of Partial Spreads
4. Decoding Linkage Codes

Outline

1 Subspace Codes

2 A Linkage Construction

3 Construction of Partial Spreads

4 Decoding Linkage Codes

Subspace Codes

Definition (Kötter/Kschischang '08 and some precursors)

- A **subspace code of length** n is a collection of subspaces in $\mathbb{F}^n$. The codewords are thus subspaces.
- If all subspaces have the same dimension, the code is a **constant dimension code.**

Random network coding:

- Packets (= vectors in $\mathbb{F}^n$) sent through a network
- Mixing at the nodes: linear combinations with unknown coefficients
- Packets are not preserved during the transmission
- Subspaces generated by packets are preserved (if no errors)

Subspace Distance

Definition

- The **subspace distance** of subspaces $\mathcal{U}, \mathcal{V} \leq \mathbb{F}^n$ is

$$\mathrm{d_S}(\mathcal{U},\mathcal{V}) = \dim(\mathcal{U}) + \dim(\mathcal{V}) - 2\dim(\mathcal{U} \cap \mathcal{V}).$$

- The **subspace distance of a subspace code** $\mathcal{C}$ is

$$\mathrm{d_S}(\mathcal{C}) = \min\{\mathrm{d_S}(\mathcal{U},\mathcal{V}) \mid \mathcal{U}, \mathcal{V} \in \mathcal{C}, \mathcal{U} \neq \mathcal{V}\}.$$

- The larger the intersection, the closer the codewords.
- $\mathrm{d_S}$ is a metric on the space of all subspaces of $\mathbb{F}^n$.

Goal:

Construct large subspace codes with large distance and efficient decoding.

Rank-Metric Codes and their Liftings

Consider $\mathbb{F}^{k \times m}$ endowed with the rank metric

$$\mathrm{d_R}(A, B) := \mathrm{rank}\,(A - B) \text{ for all } A,\ B \in \mathbb{F}^{k \times m}.$$

Definition

- **Rank-metric code with rank distance** $\mathrm{d_R}(\mathcal{M})$:
  subspace $\mathcal{M}$ of $\mathbb{F}^{k \times m}$ where

$$\mathrm{d_R}(\mathcal{M}) := \min\{\mathrm{d_R}(A, B) \mid A,\ B \in \mathcal{M},\ A \neq B\}.$$

- $\mathcal{M}$ is an **MRD code** if $|\mathcal{M}| = q^{m(k-d+1)}$ (here $k \leq m$).
- **Lifted rank-metric code:**

$$\mathcal{C} = \{\mathrm{im}\,(I \mid M) \mid M \in \mathcal{M}\},\ \text{subspace code of length } k + m.$$

Then $\mathrm{d_S}(\mathcal{C}) = 2\mathrm{d_R}(\mathcal{M})$.

Subspace Code Constructions

- Use of rank-metric codes and Ferrers diagrams:
  Kötter/Kschischang '08, Silva/Kschischang/Kötter '08, Etzion/Silberstein '09, Khaleghi/Silva/Kschischang '09, Silberstein/Etzion '11, ...
- Computer search for codes with prescribed automorphism group:
  Kohnert/Kurz '08, Braun/Reichelt '12, Braun et al. '13
- (Partial) spread codes:
  Etzion/Vardy '11, Gorla/Manganiello/Rosenthal '12, Gorla/Ravagnani '14
- Cyclic codes:
  Kohnert/Kurz '08, Etzion/Vardy '11
- Cyclic orbit codes:
  Rosenthal/Trautmann et al. '10 – '14, G_L/Morrison/Troha '14
- ...

Outline

1. Subspace Codes
2. A Linkage Construction
3. Construction of Partial Spreads
4. Decoding Linkage Codes

Linkage Codes

Theorem

For $i = 1, 2$ let $\mathcal{C}_i$ be $(n_i,\ k,\ d_i)$-constant-dimension codes with sets of representing matrices $\mathcal{M}_i \subseteq \mathbb{F}^{k \times n_i}$.

Let $\mathcal{C}_R \subseteq \mathbb{F}^{k \times n_2}$ be a rank-metric code with rank distance $\mathrm{d_R}(\mathcal{C}_R) = d_R$.

Define the linkage code

$$\mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2 := \tilde{\mathcal{C}}_1 \cup \tilde{\mathcal{C}}_2,$$

where

$$\tilde{\mathcal{C}}_1 = \{\mathrm{im}\,(\ U_1 \ \mid\ M\ ) \mid U_1 \in \mathcal{M}_1,\ M \in \mathcal{C}_R\}$$

$$\tilde{\mathcal{C}}_2 = \{\mathrm{im}\,(0_{k \times n_1} \mid\ U_2\ ) \mid U_2 \in \mathcal{M}_2\}.$$

Then $\mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2$ is a $(n_1 + n_2,\ k,\ d)$-code, where $d = \min\{d_1,\ d_2,\ 2d_R\}$, and $|\mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2| = |\mathcal{C}_1| \cdot |\mathcal{C}_R| + |\mathcal{C}_2|$.

Example: dimension 3, distance 4, length ≥ 12 over $\mathbb{F}_2$

- Use for $\mathcal{C}_R$ an MRD code of rank distance 2
- Use the largest codes of length 6 or 7, i.e., $|\mathcal{C}_1| = 77$ and $|\mathcal{C}_2| = 329$ (Kohnert/Kurz '08, Braun/Reichelt '14, Honold/Kiermaier/Kurz '14)

n	n_1	n_2	$\mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2$	ML	MML	Largest Known
12	6	6	315,469	298,139	305,324	385,515
13	7	6	1,347,661	1,192,587	1,221,296	1,597,245
14	7	7	5,390,665	4,770,411	4,885,184	5,996,178

ML=Multilevel Construction (Etzion/Silberstein '09)

MML = Modified Multilevel Construction (Trautmann/Rosenthal '10, Etzion/Silberstein '13)

Largest Known (Braun/Reichelt '14: Sophisticated Computer Search)

Outline

1 Subspace Codes

2 A Linkage Construction

3 Construction of Partial Spreads

4 Decoding Linkage Codes

Partial Spreads

Definition

- **Partial k-spread in $\mathbb{F}^n$:** constant-dimension code in $\mathbb{F}^n$ of dimension k and distance $2k$ (all subspaces intersect trivially).
- **k-spread in $\mathbb{F}^n$:** A partial k-spread where the subspaces cover $\mathbb{F}^n$.

Remark

k-spreads in $\mathbb{F}^n$ exist iff $k \mid n$. They have cardinality $\frac{q^n-1}{q^k-1}$.

Examples of k-spreads

- Orbit of $\mathbb{F}_{q^k}$ in $\mathbb{F}_{q^n}$ under the natural action of $\mathbb{F}_{q^n}^*$.
- Desarguesian spread: $(\mathbb{F}_{q^k}^m \setminus \{0\})/\mathbb{F}_{q^k}^*$, where $km = n$.

Partial Spreads

Theorem (Hong/Patel '72, Beutelspacher '75)

Let $\mu(n, k)$ be the largest possible cardinality of a partial k-spread in $\mathbb{F}^n$. Then

$$\mu(n, k) \geq \underbrace{\frac{q^n - q^c}{q^k - 1} - q^c + 1}_{=:m(n,k)}, \text{ where } c \equiv n \pmod{k}.$$

with equality if $c \in \{0, 1\}$.

Constructing Partial Spreads of Size $m(n, k)$ via Linkage

Theorem

Let $n = lk + n_2$, where $l \geq 1$ and $n_2 \geq k$ and let

- $\mathcal{C}_1$ be a k-spread in $\mathbb{F}^{lk}$,
- $\mathcal{C}_2$ be a partial k-spread in $\mathbb{F}^{n_2}$,
- $\mathcal{C}_R$ be a linear MRD code in $\mathbb{F}^{k \times n_2}$ with rank distance k.

Set $\mathcal{C} := \mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2$. Then $\mathcal{C}$ is a partial k-spread and

- If $|\mathcal{C}_2| = m(n_2, k)$, then $|\mathcal{C}| = m(n, k)$.
- If $\mathcal{C}_2$ is a maximal partial k-spread, then so is $\mathcal{C}$.

Examples of the construction

$n = n_1 + n_2$, where $n_2 = k + c$ and $n_1 = lk$.

- Etzion/Vardy '11: $\mathcal{C}_1 =$ orbit code spread in $\mathbb{F}^{n_1}$ and $|\mathcal{C}_2| = 1$.
- Gorla/Ravagnani '14: $\mathcal{C}_1 =$ Desarguesian spread in $\mathbb{F}^{n_1}$ and $|\mathcal{C}_2| = 1$.

Optimal Partial 3-Spreads over $\mathbb{F}_2$ via Linkage

Theorem (El-Zanati et al. '10)

For $q = 2,\ k = 3$, and $n \geq 6$

$$\mu(n,3) = \frac{2^n - 2^c}{7} - c = \begin{cases} m(n,3), & \text{if } c = 0, 1, \\ m(n,3) + 1, & \text{if } c = 2. \end{cases}$$

El-Zanati et al. present an optimal partial 3-spread in $\mathbb{F}_2^8$ (size $= 34$).

Theorem

Let $n \geq 10$ and write $n = 3l + n_2$ for some $l \geq 1$ and $n_2 \in \{6, 7, 8\}$. Let

- $\mathcal{C}_1$ be a 3-spread in $\mathbb{F}_2^{3l}$,
- $\mathcal{C}_2$ be an optimal partial 3-spread in $\mathbb{F}_2^{n_2}$,
- $\mathcal{C}_R$ be an MRD code in $\mathbb{F}_2^{3 \times n_2}$ with rank distance 3.

Then $\mathcal{C}_1 *_{\mathcal{C}_R} \mathcal{C}_2$ is an optimal partial 3-spread in $\mathbb{F}_2^n$.

Outline

1. Subspace Codes
2. A Linkage Construction
3. Construction of Partial Spreads
4. Decoding Linkage Codes

Decoding Linkage Codes

Theorem

- For $i=1,2$ let $n_i \geq k$ and let $\mathcal{M}_i \subseteq \mathbb{F}^{k\times n_i}$ be linear MRD codes with rank distance d.
- Let $\mathcal{C}_3 = \mathcal{C}(\mathcal{M}_3)$ and $\mathcal{C}_4 = \mathcal{C}(\mathcal{M}_4)$ be subspace codes with distance $2d$ and representing matrices $\mathcal{M}_3 \subseteq \mathbb{F}^{k\times n_1}$, $\mathcal{M}_4 \subseteq \mathbb{F}^{k\times n_2}$.

Then the code $\mathcal{C} = \mathcal{C}' \cup \mathcal{C}'' \cup \mathcal{C}'''$, where

$$
\begin{aligned}
\mathcal{C}' &= \{\mathrm{im}\,(\;I_k \;|\; M_1 \;|\; M_2\;) \mid M_1 \in \mathcal{M}_1,\, M_2 \in \mathcal{M}_2\},\\
\mathcal{C}'' &= \{\mathrm{im}\,(0_{k\times k} \mid M \mid 0_{k\times n_2}) \mid M \in \mathcal{M}_3\},\\
\mathcal{C}''' &= \{\mathrm{im}\,(0_{k\times k} \mid 0_{k\times n_1} \mid M\;) \mid M \in \mathcal{M}_4\},
\end{aligned}
$$

has length $k+n_1+n_2$, distance $2d$, and size $q^{(n_1+n_2)(k-d+1)}+|\mathcal{M}_3|+|\mathcal{M}_4|$.

Decoding reduces to decoding w.r.t. $\mathcal{C}_3$, $\mathcal{C}_4$ and the two lifted MRD codes.

$\mathcal{C}' \cup \mathcal{C}'' \cup \mathcal{C}'''$ as well as $\mathcal{C}' \cup \mathcal{C}''$ and $\mathcal{C}' \cup \mathcal{C}'''$ are linkage codes.

Decoding Linkage Codes

Theorem

- For $i = 1, 2$ let $n_i \geq k$ and let $\mathcal{M}_i \subseteq \mathbb{F}^{k\times n_i}$ be linear MRD codes with rank distance d.
- Let $\mathcal{C}_3 = \mathcal{C}(\mathcal{M}_3)$ and $\mathcal{C}_4 = \mathcal{C}(\mathcal{M}_4)$ be subspace codes with distance $2d$ and representing matrices $\mathcal{M}_3 \subseteq \mathbb{F}^{k\times n_1}$, $\mathcal{M}_4 \subseteq \mathbb{F}^{k\times n_2}$.

Then the code $\mathcal{C} = \mathcal{C}' \cup \mathcal{C}'' \cup \mathcal{C}'''$, where

$$\begin{aligned}
\mathcal{C}' &= \{\mathrm{im}\,(\;I_k \;|\; M_1 \;|\; M_2\;) \mid M_1 \in \mathcal{M}_1,\, M_2 \in \mathcal{M}_2\},\\
\mathcal{C}'' &= \{\mathrm{im}\,(0_{k\times k} \,|\; M \;|\, 0_{k\times n_2}) \mid M \in \mathcal{M}_3\},\\
\mathcal{C}''' &= \{\mathrm{im}\,(0_{k\times k} \,|\, 0_{k\times n_1} \,|\; M \;) \mid M \in \mathcal{M}_4\},
\end{aligned}$$

has length $k+n_1+n_2$, distance $2d$, and size $q^{(n_1+n_2)(k-d+1)}+|\mathcal{M}_3|+|\mathcal{M}_4|$.
Decoding reduces to decoding w.r.t. $\mathcal{C}_3$, $\mathcal{C}_4$ and the two lifted MRD codes.

$\mathcal{C}' \cup \mathcal{C}'' \cup \mathcal{C}'''$ as well as $\mathcal{C}' \cup \mathcal{C}''$ and $\mathcal{C}' \cup \mathcal{C}'''$ are linkage codes.

Decoding Linkage Codes

Theorem

- For $i = 1, 2$ let $n_i \geq k$ and let $\mathcal{M}_i \subseteq \mathbb{F}^{k \times n_i}$ be linear MRD codes with rank distance d.
- Let $\mathcal{C}_3 = \mathcal{C}(\mathcal{M}_3)$ and $\mathcal{C}_4 = \mathcal{C}(\mathcal{M}_4)$ be subspace codes with distance $2d$ and representing matrices $\mathcal{M}_3 \subseteq \mathbb{F}^{k \times n_1}$, $\mathcal{M}_4 \subseteq \mathbb{F}^{k \times n_2}$.

Then the code $\mathcal{C} = \mathcal{C}' \cup \mathcal{C}'' \cup \mathcal{C}'''$, where

$$\begin{aligned} \mathcal{C}' &= \{\mathrm{im}\,(\ I_k \ | \ M_1 \ | \ M_2\ ) \mid M_1 \in \mathcal{M}_1,\, M_2 \in \mathcal{M}_2\}, \\ \mathcal{C}'' &= \{\mathrm{im}\,(0_{k \times k} \,|\ M \ |\, 0_{k \times n_2}) \mid M \in \mathcal{M}_3\}, \\ \mathcal{C}''' &= \{\mathrm{im}\,(0_{k \times k} \,|\, 0_{k \times n_1} \,|\ M\ ) \mid M \in \mathcal{M}_4\}, \end{aligned}$$

has length $k+n_1+n_2$, distance $2d$, and size $q^{(n_1+n_2)(k-d+1)} + |\mathcal{M}_3| + |\mathcal{M}_4|$.
Decoding reduces to decoding w.r.t. $\mathcal{C}_3$, $\mathcal{C}_4$ and the two lifted MRD codes.

$\mathcal{C}' \cup \mathcal{C}'' \cup \mathcal{C}'''$ as well as $\mathcal{C}' \cup \mathcal{C}''$ and $\mathcal{C}' \cup \mathcal{C}'''$ are linkage codes.

Decoding Linkage Codes

Theorem

$$\begin{aligned}
\mathcal{C}' &= \{\mathrm{im}\,(\; I_k \;|\; M_1 \;|\; M_2 \;) \mid M_1 \in \mathcal{M}_1,\, M_2 \in \mathcal{M}_2\},\\
\mathcal{C}'' &= \{\mathrm{im}\,(0_{k\times k} \,|\; M \;|\, 0_{k\times n_2}) \mid M \in \mathcal{M}_3\},\\
\mathcal{C}''' &= \{\mathrm{im}\,(0_{k\times k} \,|\, 0_{k\times n_1} \,|\; M \;) \mid M \in \mathcal{M}_4\},
\end{aligned}$$

Let $\mathcal{V} = \mathrm{im}\,(V_0 \,|\, V_1 \,|\, V_2) \subseteq \mathbb{F}^n$ be a K-dimensional received word with $\mathrm{d_S}(\mathcal{V}, \mathcal{C}) \leq (2d-1)/2$.

Then exactly one of the following situations occurs.

- $\mathrm{rank}\,(V_0) > K/2$: Then the closest codeword in $\mathcal{C}$ is in $\mathcal{C}'$ and given by $\mathcal{U} = \mathrm{im}\,(I \,|\, M_1 \,|\, M_2)$, where $\mathrm{d_S}\big(\mathrm{im}\,(I \,|\, M_i),\, \mathrm{im}\,(V_0 \,|\, V_i)\big) \leq (2d-1)/2$.
- $\mathrm{rank}\,(V_0 \,|\, V_2) < K/2$: Then the closest codeword in $\mathcal{C}$ is in $\mathcal{C}''$ and given by $\mathcal{U} = \mathrm{im}\,(0 \,|\, M \,|\, 0)$, where $\mathrm{d_S}(\mathrm{im}\,(M),\, \mathrm{im}\,(V_1)) \leq (2d-1)/2$.
- $\mathrm{rank}\,(V_0 \,|\, V_1) < K/2$: Then the closest codeword in $\mathcal{C}$ is in $\mathcal{C}'''$ and given by $\mathcal{U} = \mathrm{im}\,(0 \,|\, 0 \,|\, M)$, where $\mathrm{d_S}(\mathrm{im}\,(M),\, \mathrm{im}\,(V_2)) \leq (2d-1)/2$.

Thank You!